(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002232451 A**
(43) Date of publication of application: **16.08.2002**

(51) Int. Cl **H04L 12/46**
G06F 13/00

(21) Application number: **2001027120**
(22) Date of filing: **02.02.2001**

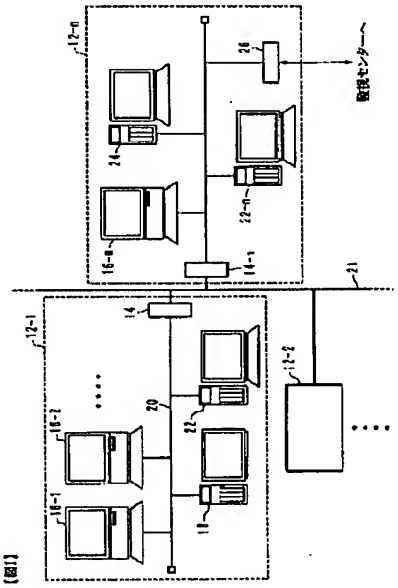
(71) Applicant: **LAYER SEVEN CO LTD**
(72) Inventor: **SUGIHARA OSAMU**
NAKAZAWA SUSUMU

(54) COMMUNICATION MANAGEMENT METHOD, COMMUNICATION MONITORING SYSTEM, AND COMPUTER SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a system that prevents internal data from being leaked or lost to the outside.

SOLUTION: A segment controller 22 in a segment demarcated by a router 14 where machines 16, 18 are interconnected via a LAN 20 acquires signal sent onto the LAN 20 and identifies a sender and a transmission destination of the acquired signal. Then the segment controller 22 discriminates whether or not the access right from the sender to the transmission destination exists, the sender is registered and a document going to be sent by the sender is a document whose transmission is inhibited or others. When there exists any trouble, the segment controller 22 requests the machine of the sender and the machine of the destination to disconnect the communication, transmits a report to a system manager to indicate occurrence of an access without the access right for the system manager and/or a warning report to the sender via the LAN 20.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－232451
（P2002－232451A）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｍ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｋ０３３
	６１０		６１０Ｑ	

審査請求　未請求　請求項の数15　ＯＬ　（全 15 頁）

(21)出願番号　特願2001－27120(P2001－27120)

(22)出願日　平成13年２月２日(2001.2.2)

(71)出願人　500093627
レイヤーセブン株式会社
東京都渋谷区渋谷３－６－２　第二矢木ビル６Ｆ

(72)発明者　杉原　修
東京都渋谷区渋谷３－６－２　第二矢木ビル６Ｆ　レイヤーセブン株式会社内

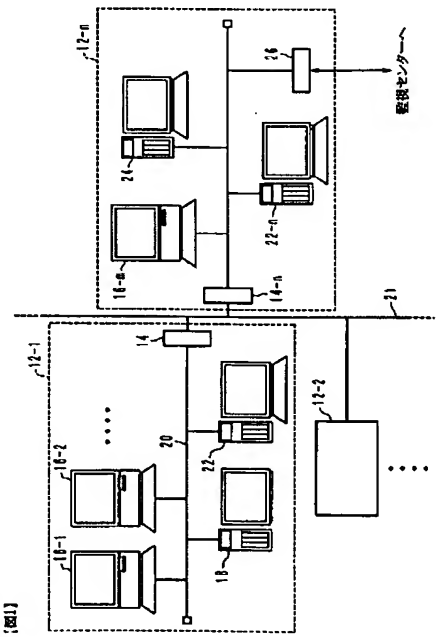
(72)発明者　中澤　進
東京都渋谷区渋谷３－６－２　第二矢木ビル６Ｆ　レイヤーセブン株式会社内

(74)代理人　100103632
弁理士　窪田　英一郎　（外１名）

最終頁に続く

(54)【発明の名称】　通信管理方法、通信監視装置、および、コンピュータシステム

(57)【要約】
【課題】　内部からのデータの流出や漏洩を防止するためのシステムを提供する。
【解決手段】　ルータ１４により画定され、かつ、複数のマシン１６、１８がＬＡＮ２０を介して接続されたセグメントにおいて、セグメントコントローラ２２が、ＬＡＮ２０上に送出された信号を取得し、取得した信号の送信元および送信先を特定する。次いで、セグメントコントローラ２２は、送信元から送信先へのアクセス権の有無や、送信元が登録されているか、送信が禁止されている文書であるか否かなどを判断する。問題がある場合には、送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者にレポートを送信し、および／または、送信元へＬＡＮ２０を介して警告レポートを送信する。



【図1】

1

【特許請求の範囲】

【請求項１】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記送信元から送信先へのアクセス権の有無を判断するステップと、

前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項２】　送信元のマシンに関するＩＰアドレスおよびポート番号、送信先のマシンに関するＩＰアドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組をデータベース中に記憶するステップを備え、

前記アクセス権の有無を判断するステップが、データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定することを特徴とする請求項１に記載の管理方法。

【請求項３】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワークに接続されたマシンのＭＡＣアドレスを登録するステップと、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記送信元のＭＡＣアドレスが登録されているか否かを判断するステップと、

前記ＭＡＣアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項４】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

2

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号がメール送信であることを判断するステップと、

前記メール送信が認められるものであるか否かを判断するステップと、

前記メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項５】　前記メール送信が認められるものであるか否かを判断するステップが、

前記信号を走査して、送信が禁止されている宛て先ではないこと、添付ファイルの有無、および／または、文字列中に禁止されたものが含まれないことを判断することを特徴とする請求項４に記載の管理方法。

【請求項６】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記信号を解析して、当該信号に基づく文字列に禁止されたものが含まれているか否かを判断するステップと、

前記信号に基づく文字列が含まれている場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項７】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

各マシンに、所定期間におけるユーザによる少なくともキー入力を蓄積するエージェントプログラムをインストールするステップと、

前記エージェントプログラムにより所定のタイミングにて、蓄積されたキー入力を示す情報を受理して、これを解析するステップと、

前記解析の結果、キー入力による文字列中に禁止されているものが含まれている場合に、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成

するステップとを備えたことを特徴とする管理方法。
【請求項８】　前記システムが、１以上のルータにより画定されたセグメントであって、当該セグメント中に１以上のマシンが配置されたセグメントを有し、各セグメントにおいて、ネットワーク上に送出された信号に基づき、前記ステップが実行されることを特徴とする請求項１ないし７の何れか一項に記載の管理方法。
【請求項９】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、
前記ネットワーク上に送出された信号を取得する信号取得手段と、
前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、
前記送信元から送信先へのアクセス権の有無を判断するアクセス権判断手段と、
前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。
【請求項１０】　さらに、送信元のマシンに関するＩＰアドレスおよびポート番号、送信先のマシンに関するＩＰアドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組を記憶したデータベースを備え、
前記アクセス権判断手段が、前記データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定することを特徴とする請求項９に記載の通信監視装置。
【請求項１１】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、
前記ネットワークに接続されたマシンのＭＡＣアドレスを登録するマシン登録手段と、
前記ネットワーク上に送出された信号を取得する信号取得手段と、
前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、
前記送信元のＭＡＣアドレスが既に登録されているか否かを判断する公式マシン判断手段と、
前記ＭＡＣアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。
【請求項１２】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、
前記ネットワーク上に送出された信号を取得する信号取得手段と、
前記取得した信号がメール送信であることを判断して、当該メール送信が認められるものであるか否かを判断するメール送信特定手段と、
前記メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。
【請求項１３】　ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、
前記ネットワーク上に送出された信号を取得する信号取得手段と、
前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、
前記信号を解析して、当該信号に基づく文字列が送信を禁止されたものであるか否かを判断する信号解析手段と、
前記文字列が送信を禁止されたものである場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。
【請求項１４】　ルータに画定されたセグメントであって、当該セグメント中に１以上のマシンが配置された、１以上のセグメントを有し、各セグメントが、請求項９ないし１３の何れか一項に記載の通信監視装置を有することを特徴とするコンピュータシステム。
【請求項１５】　各通信監視装置が、セグメント内のマシン間の通信制限に関する固有の情報と、セグメント間および外部との通信制限に関する共通の情報とを記憶したデータベースを有することを特徴とする請求項１４に記載のコンピュータシステム。
【発明の詳細な説明】
【０００１】
【産業上の技術分野】本発明は、社内からの情報の流出や漏洩を防止するシステムに関する。

【０００２】

【従来の技術】企業や組織内においては、ＬＡＮなどのネットワークによりコンピュータ（クライアントマシン）やサーバが相互に接続され、データの共有、ユーザ間のメール通信などが行われている。また、インターネットの著しい普及により、ルータおよびインターネットを介して、社内のマシンと外部のサーバ等が接続される状態となっている場合が多い。

【０００３】このように内部における相互のデータ通信や外部と内部の間のデータ通信が可能となると、外部からの侵入を防止するとともに、内部からのデータ流出や漏洩を防止することが重要となる。たとえば、インターネットを介した外部からの侵入に対してはファイアウォールを設けることである程度防止できる。したがって、企業や組織内に構築されたコンピュータシステムにおいては、外部との境界に、グローバルＩＰ領域（外部）とローカルＩＰ領域（内部）とを画定するファイアウォールを設けている。

【０００４】

【発明が解決しようとする課題】ところが、ファイアウォールでは、内部からの漏洩や流出を防止することができない。実際に、不正アクセスは、外部からの侵入よりも内部からの流出が多いのが現状である。故意にデータを持ち出すほか、不注意なメール送信等もしばしば起こり得る。さらに、ＬＡＮなど内部のネットワークに、従業者等が自身のマシンを接続することにより、当該マシンが感染しているウィルスに、内部のクライアントマシン全体が感染するというおそれもある。本発明は、内部からのデータの流出や漏洩を防止するためのシステムを提供することを目的とする。

【０００５】

【課題を解決するための手段】本発明の目的は、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、前記ネットワーク上に送出された信号を取得するステップと、前記取得した信号の送信元および送信先を特定するステップと、前記送信元から送信先へのアクセス権の有無を判断するステップと、前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法により達成される。

【０００６】本発明によれば、ローカルなネットワークを介して複数のマシンが接続されたシステムにおいて、当該ネットワーク上に送出される信号（パケット）を取得し、当該パケットに基づき、送信先および送信元を特定し、アクセス権の有無を判断している。また、アクセス権が存在しない場合には、たとえば、送信先および送信元の双方に対して、通信切断を要求する。したがって、故意或いは不注意による不正なアクセスを防止し、或いは、これを送信元や管理者に通知することが可能となる。

【０００７】本発明の好ましい実施態様においては、送信元のマシンに関するＩＰアドレスおよびポート番号、送信先のマシンに関するＩＰアドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組をデータベース中に記憶するステップを備え、アクセス権の有無を判断するステップが、データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定するように構成されている。この実施態様によれば、データの組を変更し、或いは、追加することにより、アクセス権の変化に柔軟に対応することが可能となる。

【０００８】本発明の別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、前記ネットワークに接続されたマシンのＭＡＣアドレスを登録するステップと、前記ネットワーク上に送出された信号を取得するステップと、前記取得した信号の送信元および送信先を特定するステップと、前記送信元のＭＡＣアドレスが登録されているか否かを判断するステップと、前記ＭＡＣアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。この実施態様によれば、ローカルなネットワークに接続可能なマシンを予め登録し、登録されたマシン（公式マシン）のみがネットワークを介したアクセスを認めることが可能となる。

【０００９】本発明のさらに別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、ネットワーク上に送出された信号を取得するステップと、取得した信号がメール送信であることを判断するステップと、メール送信が認められるものであるか否かを判断するステップと、メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップ

とを備えている。これにより、認められないメール送信を防止すること、或いは、メールが既に送信されてしまった場合であっても、これを管理者や送信元に知らせることが可能となる。

【００１０】より好ましい実施態様においては、メール送信が認められるものであるか否かを判断するステップが、信号を走査して、禁止された送信先であること、添付ファイルの有無、および／または、文字列中に禁止されたものが含まれないことを判断する。

【００１１】別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、ネットワーク上に送出された信号を取得するステップと、取得した信号の送信元および送信先を特定するステップと、信号を解析して、当該信号に基づく文字列に禁止されたものが含まれているか否かを判断するステップと、信号に基づく文字列が含まれている場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。

【００１２】本発明のさらに別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、各マシンに、所定期間におけるユーザによる少なくともキー入力を蓄積するエージェントプログラムをインストールするステップと、エージェントプログラムにより所定のタイミングにて、蓄積されたキー入力を示す情報を受理して、これを解析するステップと、解析の結果、キー入力による文字列中に禁止されているものが含まれている場合に、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。暗号化されたメール送信においては、ネットワークに送出されたパケットからは容易に、送信文中に問題のある文字列が含まれるか否かを判断することができない。そこで、この実施態様においては、キー入力を蓄積しておき、蓄積されたキー入力を解析して、問題のある文字列が存在したか否かを判断し、存在する場合には、これを管理者等に通知している。これにより、メール送信自体を防止できないものの、不正なメール送信が生じた可能性があること自体を知ることが可能となる。

【００１３】システムは、１以上のルータにより画定されたセグメントであって、当該セグメント中に１以上のマシンが配置されたセグメントを有し、各セグメントにおいて、ネットワーク上に送出された信号に基づき、前記ステップが実行されても良い。

【００１４】また、本発明の目的は、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、前記送信元から送信先へのアクセス権の有無を判断するアクセス権判断手段と、前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置によっても達成される。

【００１５】別の実施態様において、通信監視装置は、ネットワークに接続されたマシンのＭＡＣアドレスを登録するマシン登録手段と、ネットワーク上に送出された信号を取得する信号取得手段と、取得した信号の送信元および送信先を特定する通信マシン特定手段と、送信元のＭＡＣアドレスが既に登録されているか否かを判断する公式マシン判断手段と、ＭＡＣアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【００１６】また、別の実施態様において、通信管理装置は、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、前記信号を解析して、当該信号に基づく文字列が送信を禁止されたものであるか否かを判断する信号解析手段と、前記文字列が送信を禁止されたものである場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【００１７】さらに別の実施態様において、通信監視装置は、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号がメール送信であることを判断して、当該メール送信が認められるものであるか否かを判断するメール送信特定手段と、前記メール送信が認められないものである場合に、メールサーバに

対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【００１８】上記通信監視装置は、ルータに画定されたセグメントであって、当該セグメント中に１以上のマシンが配置された、１以上のセグメントの各々に配置されていても良い。この場合には、各通信監視装置が、セグメント内のマシン間の通信制限に関する固有の情報と、セグメント間および外部との通信制限に関する共通の情報とを記憶したデータベースを有するのが望ましい。

【００１９】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明を加える。図１は、本発明の実施の形態にかかるシステムの全体を示すブロックダイヤグラムである。この実施の形態においては、ある企業や組織内のシステム（社内システム）における内部からの情報流出を防止するために本発明を適用している。図１に示すように、この社内システムは、複数のセグメント１２－１、１２－２、・・・を有している。各セグメント（たとえばセグメント１２－１）においては、ルータ１４、クライアントマシン１６－１、１６－２、・・・、サーバ１８等が設けられている。クライアントマシンおよびサーバは、セグメント内のＬＡＮ２０にて相互に接続されている。また、ＬＡＮ２０に接続されたルータを介して他のセグメントや外部とのデータ通信も可能である。

【００２０】また、各セグメント１２には、セグメント内の通信状況を監視し、必要な場合にデータ通信の終了（マシン間の切断）などの処理を実行するセグメントコントローラ２２が設けられている。セグメントコントローラ２２は、主として、設置されたセグメント１２において、ＬＡＮ２０上で伝達されるデータ（パケット）を監視するようになっている。各セグメント１２－１、１２－２、・・・はＬＡＮ２１を介して接続され、相互にデータ通信をなすことができる。

【００２１】また、あるセグメント１２－ｎには、クライアントマシン１６－ｍなどや、セグメントコントローラ２２－ｎのほか、社内システムや、他の社内システム（図示せず）など、監視対象となるシステム全体を中央で監視する監視センターとのデータ送受信を制御する監視コンソール２４や外部ネットワーク（たとえばインターネット）との境界に配置されたルータ２６が設けられている。

【００２２】図２は、セグメントコントローラ２２の構成を示すブロックダイヤグラムである。図２に示すように、セグメントコントローラ２２は、ＬＡＮ２０上の信号（パケット）を取り入れて信号を監視する通信監視部３２と、通信監視部３２により取り込まれた信号に基づき、クライアントマシン間、クライントマシンとサーバとの間などのアクセス権の有無を判断するアクセス権管理部３４と、アクセス権等に関する種々の情報を記憶したアクセス権データベース（ＤＢ）３６と、ＬＡＮ２０上に信号を送出したマシンを特定するマシン特定部３８と、ＬＡＮ２０上に送出された信号に基づき、送信先のアドレスや信号中に含まれる文字列を特定する文字列／アドレス特定部４０と、送信を制限すべき送信先や通信文中の文字列が記憶された送信制限情報ＤＢ４２と、後述するクライアントマシン中のエージェントプログラムから、クライアントマシンへのユーザによるキー入力を示すデータを受理するキー入力受理部４４と、ユーザによるキー入力が記憶されたキー入力ＤＢ４６と、キー入力を解析するキー入力解析部４８と、必要な場合に、アクセスが行われようとしているマシン間に通信切断を求める通信切断処理部５０と、不正なアクセスなどを管理者等に通知するための処理を実行する警告土処理部５２と、アクセスログを記憶するアクセスログＤＢ５４とを有している。

【００２３】このように構成されたセグメントコントローラを利用して、本実施の形態においては、以下のような監視が実現される。

（１）アクセス制限の設定、アクセス権を伴わないアクセスの禁止、通知

（２）非公式ＰＣ（登録されていないＰＣ）のネット上での接続禁止

（３）不要なメール送信の遮断

（４）キー入力のモニターおよび解析

これらにつき、以下に説明を加える。

【００２４】（１）アクセス制限の設定等

図３および図４は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。なお、ここでは、あるクライアントマシン１６が、同一のセグメント１２内のサーバ１８にアクセスする場合につき説明を加えるが、これに限定されるものではなく、クライアントマシン間のアクセスやセグメント外の各マシンへのアクセスについても同様の処理が実行される。

【００２５】図３に示すように、クライアントマシン１６（この場合にはクライアントマシン「ａ」１６－１）から、サーバ１８（この場合にはサーバ「Ａ」１８－１）に、アクセス要求がＬＡＮ２０を介して送信された際に（ステップ３０１）、セグメントコントローラ２２の通信監視部３２は、ＬＡＮ２０上に送出されたこのアクセス要求を取得し（ステップ３０１－ｂ）、アクセス元およびアクセス先のマシンを特定する（ステップ３０２）。次いで、アクセス権管理部３４は、アクセス権ＤＢ３６を参照して、アクセス元からアクセス先へのアクセス権があるか否かを判断する（ステップ３０３）。アクセス権がある場合には、セグメントコントローラ２２は、アクセス元からアクセス先へのアクセスがあったこ

と、および、その日時を含むアクセスログを作成し、これをアクセスログＤＢ５４に記憶する（ステップ３０４）。この場合には、アクセス先であるサーバ「Ａ」１８－１は、アクセスに応答した処理を実行して（ステップ３０５）、必要なデータなどを含む応答をクライアントマシン「ａ」１６－１に返送する（ステップ３０６）。

【００２６】その一方、アクセス権がなかった場合につき図４を参照して説明を加える。ここでは、クライアントマシン１６（クライアントマシン「ａ」１６－１）が、アクセス権限のないサーバ１８（この場合にはサーバ「Ｂ」１８－２）にアクセス要求をした場合について説明する。

【００２７】図４においてステップ４０１～ステップ４０３は、図３のステップ３０１～ステップ３０３と同じである。アクセス権がないと判断された場合には（ステップ４０３参照）、セグメントコントローラ２２の通信切断処理部５０が、アクセス元のマシン（クライアントマシン「ａ」１６－１）およびアクセス先のマシン（サーバ「Ｂ」１８－２）の双方に、通信切断要求を送信する（ステップ４０４、４０５）。この通信切断要求は、アクセス先のマシンにとってはアクセス元からの切断要求と解釈され、アクセス元のマシンにとってはアクセス先からの切断要求と解釈されるようなものであるのが望ましい。

【００２８】これにより、クライアントマシン「ａ」１６－１およびサーバ「Ｂ」１８－２において通信切断の処理が実行される（ステップ４０７、４０８）。これにより、アクセス権のないマシンからのアクセスが阻止される。次いで、アクセスログがアクセスログＤＢ５４に記憶される（ステップ４０８）。また、必要に応じて、アクセス権の無いマシンからのアクセスがあったことを示す通知レポートやアクセス権の無いマシンに対するアクセスが認められなかったことを示す警告レポートが、警告通知処理部５２にて作成され、これが送信される（ステップ４０９）。たとえば、通知レポートは、監視コンソール２４に送信されれば良い。また、警告レポートはアクセス権のないアクセス先へのアクセス要求をしたマシンに送信される。

【００２９】図５は、本実施の形態におけるアクセス権ＤＢ３６に記憶されたデータの例を示す図である。図５に示すように、アクセス権ＤＢ３６においては、セグメント１２内のマシン間に関するアクセス権を規定したアクセス権情報５００と、セグメント内外を含むシステム内のアクセス権を規定したシステム内アクセス権情報５１０とが設けられている。セグメント内アクセス情報５００は、各セグメント１２に固有のものであり、各セグメント内に配置されたセグメントコントローラ２２がそれぞれ保有している。その一方、システム内アクセス権情報５１０は、全てのセグメントコントローラ２２が共通して保有している。

【００３０】たとえば、セグメント内アクセス権情報５００は、ソースマシン（アクセス元）のＩＰアドレスやポート番号からなるソースマシン情報（符号５０１参照）と、宛て先マシン（アクセス先）のＩＰアドレスやポート番号からなる宛て先マシン情報（符号５０２参照）と、ソースマシンから宛て先マシンへのアクセス制限の内容を示す制限情報（符号５０３参照）とからなるデータの組を含んでいる。アクセス制限には、たとえば、通信の切断、管理者やアクセス元ユーザへの通知、および／または、ログの記録が含まれる。アクセス権ＤＢ３６は、必要な組み合わせのデータの組を収容している。これは、必要に応じて、アクセス権管理部３４により更新され得る。

【００３１】また、システム内アクセス権情報５１０も、セグメント内アクセス情報５００のデータの組と同様の構成を有するものを含んでいる。したがって、これを参照することにより、セグメント外へのアクセスや、たとえばインターネットを介するシステム外へのアクセスに関するアクセス権の有無を判断することもできる。

【００３２】アクセス権の有無を判断する処理（図３のステップ３０３、図４のステップ４０３）においては、アクセス権管理部３４が、アクセス権ＤＢ３６を検索して、当該ソースマシン（アクセス元）に関して、宛て先マシンおよびアクセス制限がどのようになっているかを特定すれば良い。

【００３３】このように、本実施の形態においては、セグメント内のアクセス、セグメント間のアクセス、さらには、システム外へのアクセスについて、セグメントコントローラがセグメント中のＬＡＮ上を通る信号を監視し、必要な場合には、アクセス制限にしたがって、通信の切断などの処理を実行する。したがって、認められてないアクセスを防止することが可能となる。

【００３４】（２）非公式ＰＣのアクセス禁止

また、本実施の形態においては、予め登録されたマシン以外のマシンによる他のマシンへのアクセスを禁止できるようになっている。たとえば、ユーザが個人のマシンを持参してＬＡＮ２０に接続する場合がある。このようなときに、個人のマシンがウィルスに感染していたり、何らかのトラブルが生じていると、当該個人のマシンによるアクセスによって、他のマシンにも障害が生じるおそれがある。また、個人のマシンに情報がダウンロードされることにより、社外秘など秘密保持すべき情報が外に持ち出されるおそれもある。本実施の形態においては、このようなアクセスを制限し、他のマシンへの障害や情報の持ち出し等を適切に防止する。

【００３５】このために、セグメントコントローラ２２は、たとえば、セグメント１２中に配置されＬＡＮ２０と接続されているクライアントマシン１６やサーバ１８の、それぞれのＭＡＣアドレスをアクセス権ＤＢ３６に

記憶しておくのが望ましい。図６は、予め登録されていないクライアントマシン（非公式クライアントマシン）によるアクセスの際に実行される処理を示すフローチャートである。図６に示すように、非公式クライアントマシンから、たとえば、あるサーバ１８（この場合にはサーバ「Ａ」１８－１）に、アクセス要求がＬＡＮ２０を介して送信された際に（ステップ６０１）、セグメントコントローラ２２の通信管理部３２は、ＬＡＮ２０上に送出されたこのアクセス要求を取得する（ステップ６０１－ｂ）。

【００３６】次いで、マシン特定部３８は、アクセス元のＭＡＣアドレスを特定し、アクセス権ＤＢ３６を検索して、当該ＭＡＣアドレスが登録されているものか否か、つまり、アクセス元が公式マシンか否かを判断する（ステップ６０２）。ＭＡＣアドレスが登録されている場合には（ステップ６０２でイエス(Yes)）、図３のステップ３０４と略同様の処理が実行される。その一方、ステップ６０２にてノー(No)と判断された場合には、アクセス元である非公式クライアントマシンおよびアクセス先のマシン（サーバ「Ａ」１８－１）の双方に、通信切断要求を送信する（ステップ６０３、６０４）。これにより、非公式クライアントマシンおよびサーバ「Ｂ」１８－２において通信切断の処理が実行される（ステップ６０５、６０６）。これにより、非公式マシンからのアクセスが阻止される。

【００３７】次いで、アクセスログがアクセスログＤＢ５４に記憶される（ステップ６０７）。また、必要に応じて、非公式マシンからのアクセスがあったことを示す通知レポートや非公式マシンに対するアクセスが認められなかったことを示す警告レポートが、警告通知処理部５２にて作成され、これが送信される（ステップ６０８）。

【００３８】（３）不要なメール送信の遮断

さらに、本実施の形態においては、認められていないメール送信を阻止するための処理を実行することもできる。これは、ＬＡＮ上に送出されたメールを監視することにより実現される。図７は、メール送信の遮断処理を示すフローチャートである。図７に示すように、あるクライアントマシン（この場合にはクライアントマシン「ａ」１６－１）からメール（メールのパケット）が送信されたときに、セグメントコントローラ２２の通信管理部３２は、ＬＡＮ２０上に送出されたメールのパケットを取得し（ステップ７０１－ｂ）、文字列／アドレス特定部４０が、当該メールがメールサーバを介して送信先に送信すべきものであるか否かを判断する（ステップ７０２）。

【００３９】図８は、本実施の形態におけるステップ７０２のメール送信許可判断処理を示すフローチャートである。図８に示すように、セグメントコントローラ２２の文字列／アドレス特定部４０は、まず、メールの送信元および送信先を特定する（ステップ８０１）。本実施の形態においては、送信制限情報ＤＢ４２に、送信先の制限に関する情報、添付ファイルの送信の認否などを示す情報が記憶されている。たとえば、マシンごとにメール送信先の制限、添付ファイルの認否が設定され、その情報が記憶されていても良い。たとえば、これにより、マシンごとに事前に登録した送信先以外のメール送信を禁止し、或いは、所定の送信先に宛てたメール送信を禁止することができる。或いは、一括して送信が認められないメール送信先が設定され、或いは、添付ファイルが認められないことなどが設定あせれていても良い。

【００４０】さらに、本実施の形態においては、メールの送信文を走査して、認められていない文字列を検出することができるようになっている。文字列／アドレス特定部４０は、送信元のマシンが特定されると、送信が認められたメールの送信先であるか否か（ステップ８０２）、添付ファイルの有無（ステップ８０３）および禁止された文字列が送信文中に含まれるか否か（ステップ８０４）を判断し、これらの条件が合致する場合（全てのステップでノー(No)）の場合に、メール送信を許可する（ステップ７０２にてイエス(Yes)）。メール送信が認められる場合には、図３のステップ３０４以降の処理が実行される。

【００４１】その一方、ステップ８０２～８０４の何れかにおいてイエス（Yes）と判断されると、送信を許可すべきでないと判断され（ステップ７０２にてノー(No)）、その結果、メール不送信要求が作成され（ステップ８０５）、これがメールサーバに送信される（ステップ７０３）。これにより、メールサーバにおいては、メール送信が中止される（ステップ７０４）。

【００４２】また、アクセスログがアクセスログＤＢ５４に記憶され（ステップ７０５）、かつ、送信が認められていない送信先等へのメール送信があったことを示す通知レポートや、送信元のマシンに対する警告レポートが、警告通知処理部５２にて作成され、これが、それぞれ管理者や送信元のマシンに向けて送信される（ステップ７０６）。たとえば、短い送信文の場合には、メールサーバを介して既に送信先に送信されてしまっている可能性もある。したがって、ここでは通知レポートの作成および管理者への通知が行われることが望ましい。

【００４３】（４）キー入力のモニターおよび解析

上述したように、本実施の形態では、メール送信文に含まれる文字列を走査して、禁止された文字列が含まれているか否かが判断される。しかしながら、メール本文を暗号化して送信する場合については、これを復号して、問題のあるメール送信を阻止することは困難である。そこで、本実施の形態においては、クライアントマシン１６の各々にエージェントプログラムを予めインストールして、エージェントプログラムが、ユーザのキーストロークを蓄積している。蓄積されたキーストロークのデー

タは、セグメントコントローラ２２において解析され、問題のある入力があるか否かが調べられる。これにより、事後的ではあるが、秘密保持すべき情報の漏洩があったか否かなどを知ることが可能となる。

【００４４】図９は、本実施の形態にかかるキーストローク解析の処理を示すフローチャートである。クライアントマシン１６のエージェントプログラムは、ユーザのキーストロークを蓄積する（ステップ９０１）。所定の期間（たとえば１日）だけ蓄積されたキーストローク情報は、所定のタイミングで、当該クライアントマシン１６が配置されたセグメント１２中のセグメントコントローラ２２に伝達される（ステップ９０２）。

【００４５】セグメントコントローラ２２がキーストローク情報を受理すると、キー入力受理部４４が、これをユーザと関連付けてキー入力ＤＢ４６に記憶する（ステップ４０３）。次いで、キー入力解析部４８は、キー入力ＤＢ４６中のキーストローク情報を読み出して、これを解析する（ステップ９０４）。この解析においては、たとえば、押下されたキーの組み合わせから、禁止された文字列が含まれるか否かなどが判断される（ステップ９０５）。キーストロークに基づく解析の結果、何らかの問題が生じている場合には（ステップ９０５でイエス(Yes)）、監視コンソール２４の管理者に向けて、通知レポートを作成して送信する（ステップ９０６）。この通知レポートにおいては、クライアントマシン名、ユーザ名、解析の結果生じていたと考えられる問題点が記述されれば良い。これにより、事後的に、クライアントマシンのユーザによる問題のあるキー入力を知ることができる。

【００４６】本実施の形態にかかる監視コンソール２４においては、セグメントコントローラ２２からの通知レポート等を受理して、これを表示装置の画面上に表示できるようになっている。図１０は、監視コンソール２４の表示装置の画面上に表示された画像例を示す図である。図１０（ａ）に示すように、監視コンソール２４の表示装置の画面上には、システム中のマシン（クライアントマシン１６、サーバ１８など）およびＬＡＮの接続形態が表示される。図１０（ａ）において、たとえば、符号１００２にて示すものがマシンを表し、符号１００３にて示すものがＬＡＮを表す。ここで、セグメントコントローラ２２により、あるセグメント中のマシンにおいて、（１）～（４）にて説明した問題（アクセス権の無いマシンへのアクセス、非公式マシンによるアクセス、禁止されたメール送信、キー入力における問題）が生じていると判断され、通知レポートが、監視コンソール２４に与えられた場合には、当該問題が生じたマシンが、たとえば、点滅するなど他のマシンと区別して表示される（符号１００４参照）。

【００４７】監視コンソール２４の操作者（管理者）は、マウスなどの入力装置を操作して、図１０（ａ）の画像中の問題が生じたマシンを指定することにより、図１０（ｂ）に示すように、通知レポートに含まれた情報から生成された画像を表示装置の画面上に表示させることができる。この画像には、たとえば、マシン名、ユーザ名、問題が発生した日時、その種別および内容、並びに、問題に対する処置が含まれる。これにより、管理者は、システム中のどのマシンに問題が生じているかをリアルタイムに把握することができる。

【００４８】また、入力装置を操作してマシンを指定して、ログの表示コマンドを入力することにより、当該マシンのログを表示することができる。このログは、マシンが配置されたセグメント中のセグメントコントローラから、必要に応じて送信されても良い。或いは、セグメントコントローラが所定のタイミングで、セグメント中のマシンのログを監視コンソールに伝達し、これを監視コンソールがＤＢ中に記憶しておき、必要に応じて、ＤＢを読み出すように構成しても良い。

【００４９】さらに、監視コンソール２４は、外部ネットワークを介して、監視センターに必要なレポート（たとえば月次レポート）を送信することもできる。また、特に必要な場合（単に、問題のあるアクセスを検出するだけでなく、何らかの特別な対策を講じるべき場合など）には、監視センターに、問題のあるアクセスに関するレポートを送信して、対応策を仰ぐことも可能である。

【００５０】本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。たとえば、前記実施の形態においては、システム内を複数のセグメントに分割し、セグメントごとにセグメントコントローラを配置し、基本的に、セグメント内のマシンのアクセスに関してはセグメントコントローラが監視および必要な処置を施すように構成しているが、これに限定されるものではなく、システム内を単一のセグメントから構成し、これを単一のセグメントコントローラがマシンを監視等するようにしても良い。なお、この場合には、セグメントコントローラおよび監視コンソールを一体として形成するのが望ましい。

【００５１】また、前記実施の形態において、何らかの問題のあるアクセス（アクセス権の無いアクセス、非公式マシンによるアクセス、問題のあるメール送信）について、通信切断および通知レポートの作成の処理を実行しているが、これに限定されるものではない。これら処置は、マシンごと、ＩＰアドレスごとに、必要な処置を設定しておき、設定された条件にしたがって、必要な処理を実行すればよい。

【００５２】さらに、前記実施の形態において、文字列／アドレス特定部４０は、メール送信にかかる信号を解析して、当該信号により特定される文字列にて禁止され

ているものが含まれているか否かを判断しているが、これに限定されるものではない。たとえば、ＬＡＮ上に送出されたパケットを取得し、これらのパケット中に禁止された文字列が含まれるか否かを判断するように構成しても良い。すなわち、ＷＥＢ閲覧、ＦＴＰによるファイル転送、ＴＥＬＮＥＴなどの全ての操作に対して、当該操作やそのための文字列をモニターして、禁止された操作や文字列の送信を防止することも可能である。なお、本明細書において、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【００５３】

【発明の効果】本発明によれば、内部からのデータの流出や漏洩を防止するためのシステムを提供することが可能となる。

【図面の簡単な説明】

【図１】　図１は、本発明の実施の形態にかかるシステムの全体を示すブロックダイヤグラムである。

【図２】　図２は、本実施の形態にかかるセグメントコントローラの構成を示すブロックダイヤグラムである。

【図３】　図３は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。

【図４】　図４は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。

【図５】　図５は、本実施の形態におけるアクセス権ＤＢに記憶されたデータの例を示す図である。

【図６】　図６は、本実施の形態において、非公式クライアントマシンによるアクセスの際に実行される処理を＊示すフローチャートである。

【図７】　図７は、本実施の形態にかかるメール送信の遮断処理を示すフローチャートである。

【図８】　図８は、本実施の形態におけるメール送信許可判断処理を示すフローチャートである。

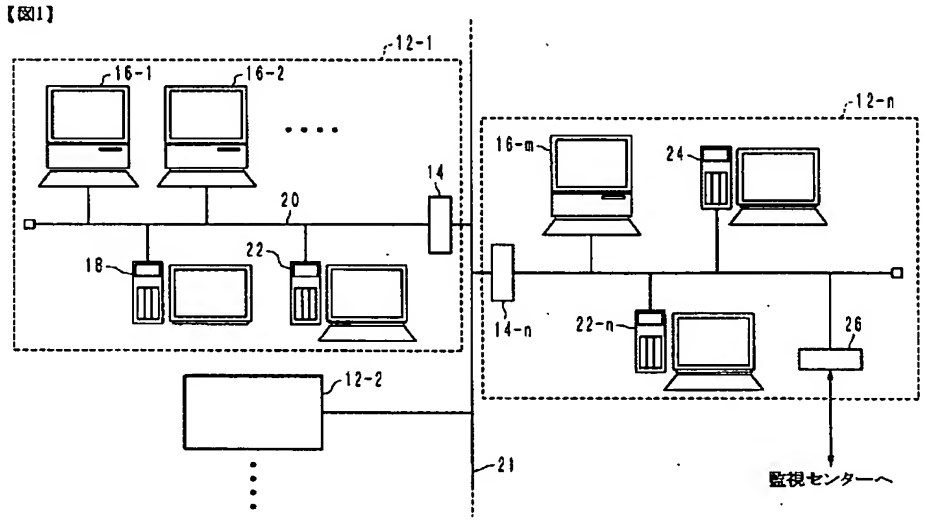
【図９】　図９は、本実施の形態にかかるキーストローク解析の処理を示すフローチャートである。

【図１０】　図１０は、本実施の形態にかかる監視コンソールの表示装置の画面上に表示された画像例を示す図である。

【符号の説明】

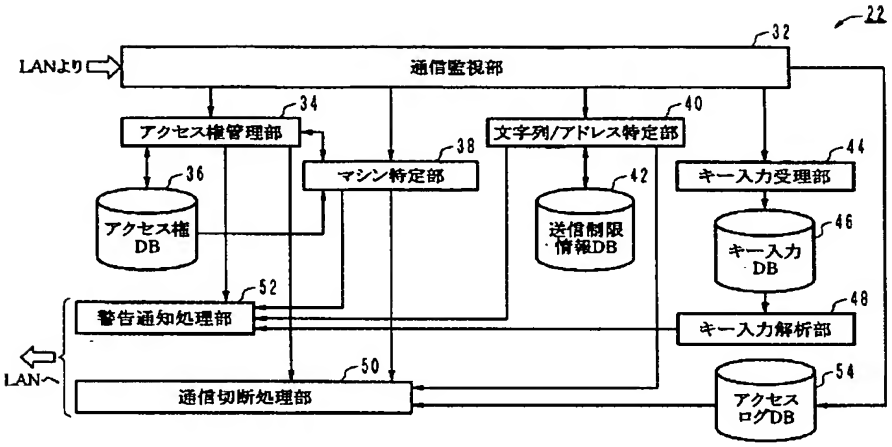
１２	セグメント
１４	ルータ
１６	クライアントマシン
１８	サーバ
２０	ＬＡＮ
２２	セグメントコントローラ
２４	監視コンソール
３２	通信管理部
３４	アクセス権管理部
３６	アクセス権ＤＢ
３８	マシン特定部
４０	文字列／アドレス特定部
４２	送信制限情報ＤＢ
４４	キー入力受理部
４６	キー入力ＤＢ
４８	キー入力解析部
５０	通信切断処理部
５２	警告通信処理部

【図１】



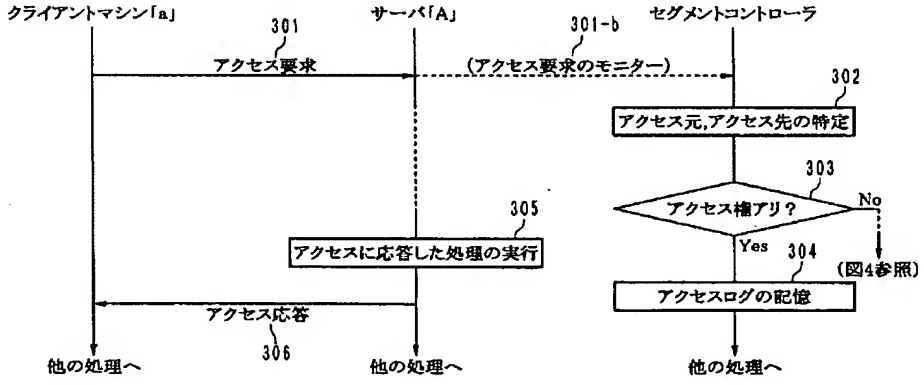
【図２】

【図2】


22
32
LANより
通信監視部
34
アクセス権管理部
40
文字列/アドレス特定部
38
マシン特定部
44
キー入力受理部
36
アクセス権DB
42
送信制限情報DB
46
キー入力DB
52
警告通知処理部
48
キー入力解析部
LANへ
50
通信切断処理部
54
アクセスログDB

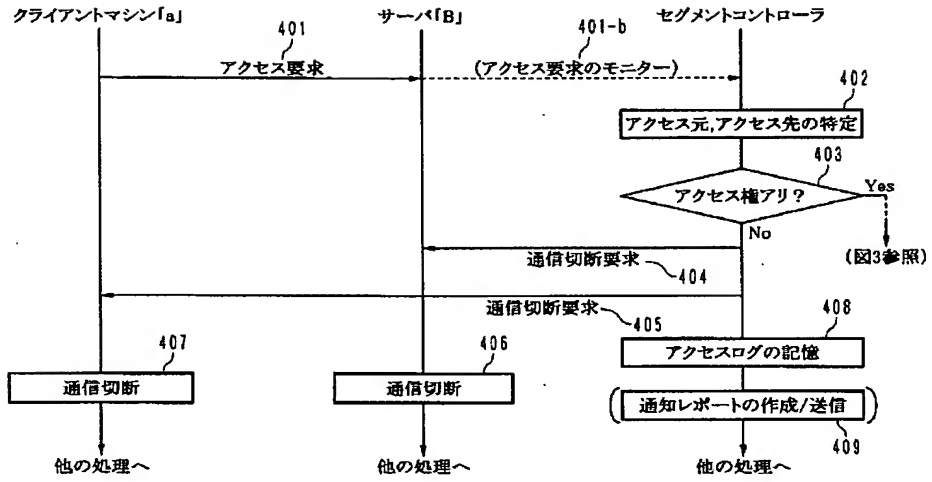
【図３】

【図3】


クライアントマシン「a」
サーバ「A」
セグメントコントローラ
301
アクセス要求
301-b
(アクセス要求のモニター)
302
アクセス元,アクセス先の特定
303
アクセス権アリ?
No
Yes
(図4参照)
305
アクセスに応答した処理の実行
304
アクセスログの記憶
アクセス応答
306
他の処理へ
他の処理へ
他の処理へ

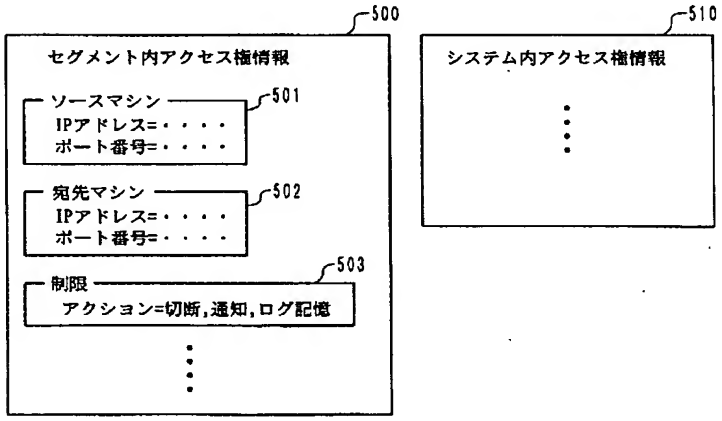
【図４】

【図4】


クライアントマシン「a」
サーバ「B」
セグメントコントローラ
401
アクセス要求
401-b
(アクセス要求のモニター)
402
アクセス元,アクセス先の特定
403
アクセス権アリ？
Yes
No
(図3参照)
通信切断要求
404
通信切断要求
405
408
アクセスログの記憶
407
406
通信切断
通信切断
通知レポートの作成/送信
409
他の処理へ
他の処理へ
他の処理へ

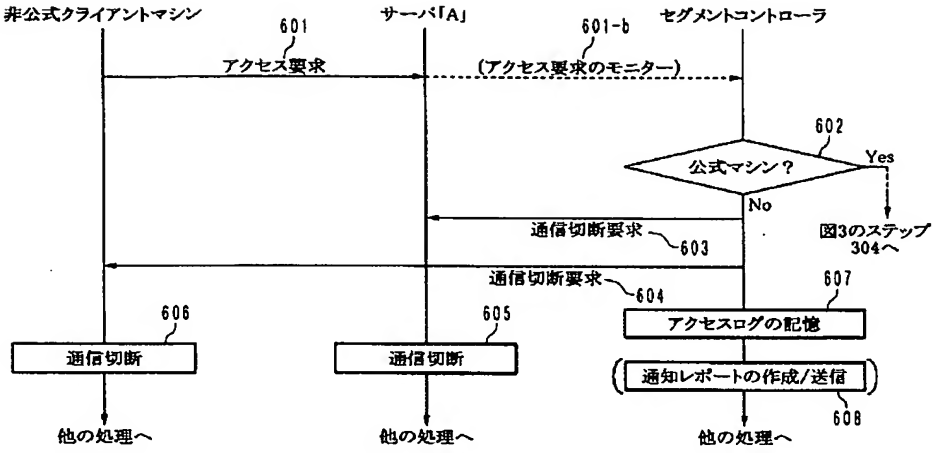
【図５】

【図5】


500
セグメント内アクセス権情報
ソースマシン
IPアドレス=・・・・
ポート番号=・・・・
501
宛先マシン
IPアドレス=・・・・
ポート番号=・・・・
502
制限
アクション=切断,通知,ログ記憶
503
510
システム内アクセス権情報

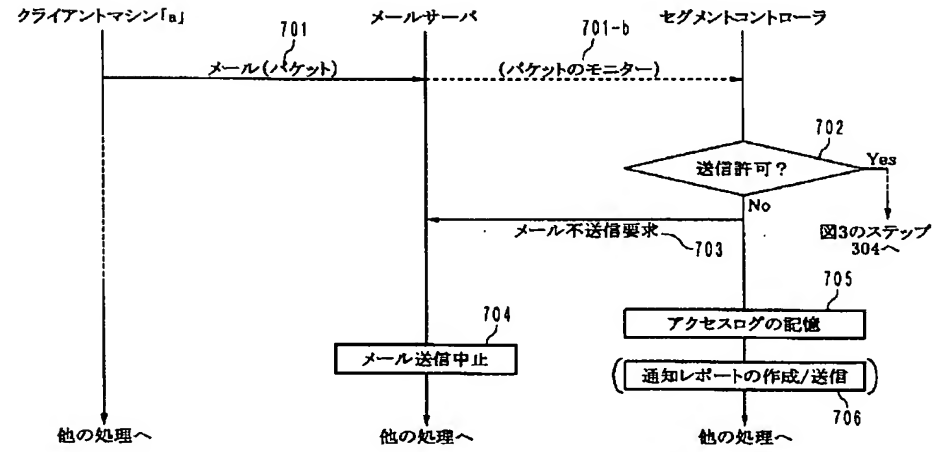
【図６】

【図6】


非公式クライアントマシン
サーバ「A」
セグメントコントローラ
601
アクセス要求
601-b
(アクセス要求のモニター)
602
公式マシン？
Yes
No
図3のステップ304へ
通信切断要求
603
通信切断要求
604
607
アクセスログの記憶
606
605
通信切断
通信切断
通知レポートの作成/送信
608
他の処理へ
他の処理へ
他の処理へ

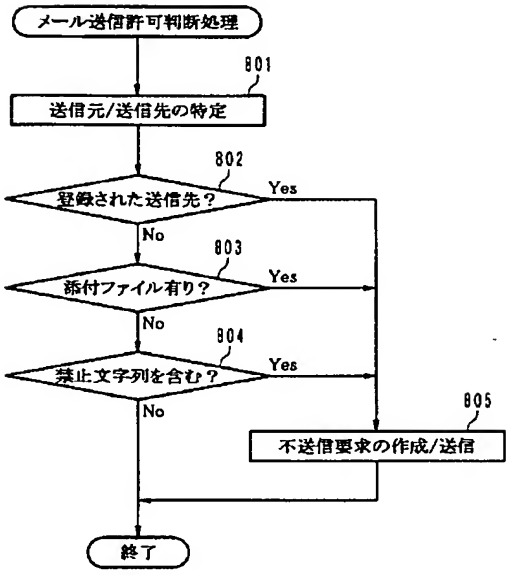
【図７】

【図7】


クライアントマシン「a」
メールサーバ
セグメントコントローラ
701
メール(パケット)
701-b
(パケットのモニター)
702
送信許可？
Yes
No
図3のステップ304へ
メール不送信要求
703
705
704
アクセスログの記憶
メール送信中止
通知レポートの作成/送信
706
他の処理へ
他の処理へ
他の処理へ

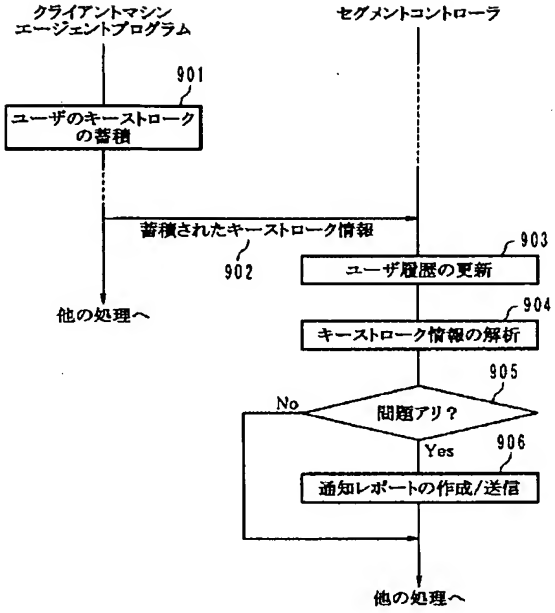
【図８】

【図8】


メール送信許可判断処理
801
送信元/送信先の特定
802
登録された送信先？
Yes
No
803
添付ファイル有り？
Yes
No
804
禁止文字列を含む？
Yes
No
805
不送信要求の作成/送信
終了

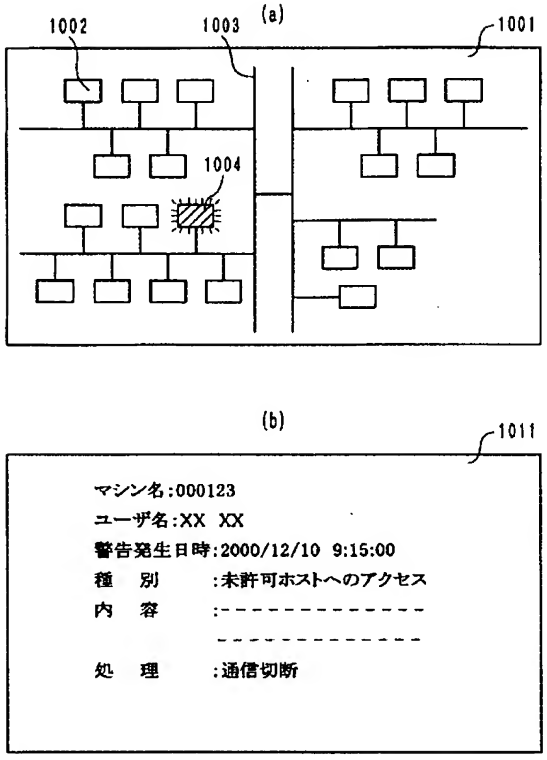
【図９】

【図9】


クライアントマシン
エージェントプログラム
セグメントコントローラ
901
ユーザのキーストローク
の蓄積
蓄積されたキーストローク情報
902
903
ユーザ履歴の更新
他の処理へ
904
キーストローク情報の解析
905
No
問題アリ？
Yes
906
通知レポートの作成/送信
他の処理へ

【図１０】

【図10】



フロントページの続き

Ｆターム(参考) 5B089 GA31 GB02 JA31 KA17 KB13
KC52 KC54
5K033 AA08 CB08 DA01 DA05 DB19
EA06 EA07 EC04